Claims

What is claimed is:

1. A biometrically secured memory IC comprising:

a sensing device for receiving biometric information provided thereto and for providing a signal indicative of the biometric information;

an integrated circuit irremovably bonded to the sensing device such that the sensing device and the integrated circuit form a single physical unit, the integrated circuit comprising:

an A/D converter for receiving the signal indicative of the biometric information and for providing digital data indicative of the signal;

first memory for storing first digital data, wherein the first digital data comprise digital data indicative of biometric information of an authorized user of the memory IC;

second memory for storing second digital data, wherein the second digital data comprise other digital data than digital data indicative of biometric information of the authorized user;

a processor for receiving the digital data indicative of the biometric information, for comparing the digital data indicative of the biometric information with the first digital data to produce a comparison result, and if the comparison result is indicative of a match for providing access to the second memory; and,

a port for providing and/or receiving the second digital data.

2. A biometrically secured memory IC as defined in claim 1, wherein the biometric information is fingerprint information.

3. A biometrically secured memory IC as defined in claim 2, wherein the integrated circuit comprises circuitry such that the second digital data stored in the second memory is only accessible if the processor provides access.

4. A biometrically secured memory IC as defined in claim 3, wherein the integrated circuit is irremovably bonded to the sensing device such that separation of the sensing device from the integrated circuit results in destruction of the integrated circuit erasing the second digital data.

5. A biometrically secured memory IC as defined in claim 3, wherein the port comprises a socket for removably joining the biometrically secured memory IC to an electronic device and wherein the socket is irremovably bonded to the integrated circuit.

6. A biometrically secured memory IC as defined in claim 5, wherein the socket is capable of mating with the socket of a second other biometrically secured memory IC for securely transmitting the second data to the second other biometrically secured memory IC in order to replace the biometrically secured memory IC.

7. A biometrically secured memory IC as defined in claim 6, wherein the processor of the biometrically secured memory IC and a processor of the second other biometrically secured memory IC comprise circuitry for identifying the second biometrically secured memory IC as a valid device before transmission of the second data.

8. A biometrically secured memory IC as defined in claim 5, wherein the integrated circuit, the sensing device and the socket form a physical unit such that an attempt by an unauthorized person to access the second digital data results in erasing of the digital data stored within the memory.

9. A biometrically secured memory IC as defined in claim 3, wherein the processor comprises circuitry for processing the second digital data if the comparison result is indicative of a match.

10. A biometrically secured memory IC as defined in claim 9, wherein the processor comprises circuitry for encrypting/decrypting at least a portion of the second digital data.

11. A biometrically secured memory IC comprising:

a capacitive fingerprint imager for receiving fingerprint information provided thereto and for providing a signal indicative of the fingerprint information;

an integrated circuit irremovably bonded to the capacitive fingerprint imager such that the capacitive fingerprint imager and the integrated circuit form a single physical unit, the integrated circuit comprising:

an A/D converter for receiving the signal indicative of the fingerprint information and for providing digital data indicative of the signal;

first non-volatile memory for storing first digital data, wherein the first digital data comprise digital data indicative of fingerprint information of an authorized user of the memory IC;

second memory for storing second digital data, wherein the second digital data comprise other digital data than digital data indicative of fingerprint information of the authorized user;

a processor for receiving the digital data indicative of the fingerprint information, for comparing the digital data indicative of the fingerprint information with the first digital data to produce a comparison result, and if the comparison result is indicative of a match for providing secured access to the second memory; and,

a port for providing and/or receiving the second digital data.

12. A biometrically secured memory IC as defined in claim 11, wherein the second memory comprises RAM.

13. A biometrically secured memory IC as defined in claim 11, wherein the second memory comprises ROM.

14. A biometrically secured memory IC as defined in claim 11, wherein the processor comprises circuitry for providing secured access, the secured access comprising only one of read or write access, and wherein the other is available without authorization.

15. A biometrically secured memory IC as defined in claim 11, wherein the port comprises a transmitter for wireless transmission of the second digital data, the transmitter being a portion of the integrated circuit.

16. A method for copying digital data to a void biometrically secured memory IC comprising the steps of:

a) establishing a trusted communication link between a first biometrically secured memory IC and a second biometrically secured memory IC, wherein each of the first and the second biometrically secured memory IC comprise a biometric sensing device and an integrated circuit, which is irremovably bonded to the biometric sensing device such that the biometric sensing device and the integrated circuit form a single physical unit;

b) transmitting first digital data indicative of biometric information of an authorized user of the first biometrically secured memory IC from first memory of the first biometrically secured memory IC to first memory of the second biometrically secured memory IC for storage therein; and,

c) transmitting second digital data from second memory of the first biometrically secured memory IC to second memory of the second biometrically secured memory IC for storage therein, wherein the second digital data comprise other digital data than digital data indicative of biometric information of an authorized user.

17. A method for copying digital data to a void biometrically secured memory IC as defined in claim 16, wherein the step of establishing a trusted communication link comprises mating of a connector of the first biometrically secured memory IC with a respective connector of the second biometrically secured memory IC.

18. A method for copying digital data to a void biometrically secured memory IC as defined in claim 17, comprising the steps of:

capturing biometric information provided to the biometric sensing device of the second biometrically secured memory IC, the biometric sensing device providing a signal indicative of the sensed biometric information;

converting the signal indicative of the sensed biometric information into captured digital data using an A/D converter integrated in the integrated circuit of the second biometrically secured memory IC;

transmitting the captured digital data to the first biometrically secured memory IC;

using a processor integrated in the integrated circuit of the first biometrically secured memory IC, comparing the captured digital data with the first digital data stored in the first memory of the first biometrically secured memory IC to produce a comparison result; and,

if the comparison result is indicative of a match, communicating with a processor integrated in the integrated circuit of the second biometrically secured memory IC for preparing the transmission of the first and the second digital data.

19. A method for copying digital data to a void biometrically secured memory IC comprising the steps of:

a) mating a connector of a first biometrically secured memory IC with a first connector of a trusted peripheral device, wherein the first biometrically secured memory IC comprises a biometric sensing device and an integrated circuit, which is irremovably bonded to the biometric sensing device such that the biometric sensing device and the integrated circuit form a single physical unit;

b) mating a connector of a second biometrically secured memory IC with a second connector of the trusted peripheral device, wherein the second biometrically secured memory IC comprises a biometric sensing device and an integrated circuit, which is irremovably bonded to the biometric sensing device such that the biometric sensing device and the integrated circuit form a single physical unit;

c) establishing a trusted communication link between a first biometrically secured memory IC and a second biometrically secured memory IC;

d) transmitting first digital data indicative of biometric information of an authorized user of the first biometrically secured memory IC from first memory of the first biometrically secured memory IC to first memory of the second biometrically secured memory IC for storage therein; and,

e) transmitting second digital data from second memory of the first biometrically secured memory IC to second memory of the second biometrically secured memory IC for storage therein, wherein the second digital data comprise other digital data than digital data indicative of biometric information of an authorized user.

20. A method for copying digital data to a void biometrically secured memory IC as defined in claim 19, comprising the steps of:

capturing biometric information provided to a biometric sensing device, the biometric sensing device providing a signal indicative of the sensed biometric information;

converting the signal indicative of the sensed biometric information into captured digital data;

comparing the captured digital data with the first digital data stored in the first memory of the first biometrically secured memory IC to produce a comparison result; and,

if the comparison result is indicative of a match, preparing the transmission of the first and the second digital data.

21. A method for copying digital data to a void biometrically secured memory IC as defined in claim 20, wherein the biometric information is captured using a biometric sensing device of the trusted peripheral device.

22. A method for copying digital data to a void biometrically secured memory IC as defined in claim 21, wherein the signal indicative of the sensed biometric information is converted into captured digital data using an A/D converter of the trusted peripheral device.

23. A method for copying digital data to a void biometrically secured memory IC as defined in claim 22, wherein the captured digital data is compared with the first digital data stored in the first memory of the first biometrically secured memory IC using a processor of the trusted peripheral device.